Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claims 1-32 (canceled)

Claim 33 (new): A method for cryptographically processing data, comprising the steps of:
a) feeding, to a cryptographic process (P), values of data (X) and a key (K);
b) performing the cryptographic process (P) to yield cryptographically processed output data (Y);
c) feeding, to the process (P), auxiliary values that mask the data (X) used in the process (P); and
d) compensating, by an auxiliary process, influence of the auxiliary values on the output data (Y).

Claim 34 (new): A method for cryptographically processing data, comprising the steps of:
a) feeding, to a cryptographic process (P), values of data (X) and a key (K);
b) performing the cryptographic process (P) to yield cryptographically processed output data (Y);
c) feeding, to an invertible supplementary process (P*), a supplementary key (K*) in order to form the key (K); and
d) wherein:
the supplementary key (K*) masks the key (K) used in the process (P); and

the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

Claim 35 (new): The method recited in claim 34 wherein the supplementary key (K*) is obtained from a process that is inverse to the supplementary process (P*) and based on the key (K) and the auxiliary key (K').

Claim 36 (new): A method for cryptographically processing data, comprising the steps of:

a) feeding, to a cryptographic process (P), values of data (X) and a key (K);

b) performing the cryptographic process (P) in order to form cryptographically processed output data (Y);

c) feeding, to an supplementary process (P*), a supplementary key (K*) in order to form the key (K);

d) wherein:

the supplementary key (K*) masks the key (K) used in the process (P);

the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed;

the data (X) is also fed to the supplementary process (P*); and

the supplementary process (P*) is performed only if the data (X) has predetermined properties.

Claim 37 (new): The method recited in claim 33 wherein the cryptographic process (P) comprises a number of steps (S_i), each of said steps (S_i) having a cryptographic operation for processing right-hand data (RD_i) derived from the data (X), so as to yield processed right-hand data (FD_i), and a combinatory operation (CC_i) for combining with left-hand

data (LD_i), also derived from the data (X), and the processed right-hand data (FD_i) in order to form modified left data (SD_i'), and wherein right-hand data (RD_1) is combined with a primary auxiliary value (A_1) prior to a first one of the steps (S_1) and left-hand data (LD_1) is combined with an additional auxiliary value (A_0).

Claim 38 (new): The method recited in claim 37 wherein immediately after a last one of the steps (S_n), right-hand data (RD_n) is combined with a further primary auxiliary value (A_n) and modified left-hand data (SD_n') is combined with a further additional auxiliary value (A_{n+1}).

Claim 39 (new): The method recited in claim 37 wherein the right-hand data (RD_i) is combined, in each one of the steps (S_i) and prior to a cryptographic operation (F_i), with a primary auxiliary value (A_i) of said one step (S_i).

Claim 40 (new): The method recited in claim 37 wherein the processed right-hand data (FD_i) is combined, following a cryptographic operation (F_i), with a secondary auxiliary value (B_i) of said one step (S_i).

Claim 41 (new): The method recited in claim 40 wherein the secondary auxiliary value (B_i) of one of the steps (S_i) is formed from a combination of a primary auxiliary value (A_{i-1}) of a preceding one of the steps and a primary auxiliary value (A_{i+1}) of a next one of the steps.

Claim 42 (new): The method recited in claim 37 wherein all primary auxiliary values (A_i) are equal.

Claim 43 (new): The method recited in claim 38 wherein the primary auxiliary values (A_i) or secondary auxiliary values (B_i) have been previously combined each time with a respective cryptographic operation (F_i').

Claim 44 (new): The method recited in claim 43 wherein a combined cryptographic operation (F_i') contains a plurality of tables; and the tables are determined in a different order each time the cryptographic process (P) is performed.

Claim 45 (new): The method recited in claim 43 wherein a combined cryptographic operation (F_i') contains a plurality of tables; and the elements of the tables are determined or stored in a different order each time the cryptographic process (P) is performed.

Claim 46 (new): The method recited in claim 45 wherein the order is stored as a lookup table.

Claim 47 (new): The method recited in claim 37 wherein the right-hand data (RD_i) is combined with a tertiary auxiliary value (W_i) after each one of the steps (S_i).

Claim 48 (new): The method recited in claim 47 wherein the tertiary auxiliary value (W_i) in all steps, except the last one of said steps (S_n), equals a combination of the primary auxiliary value (A_1) of the first one of the steps (S_1) and the additional auxiliary value (A_0); and in the last one of the steps (S_n) the tertiary auxiliary value equals zero.

Claim 49 (new): The method recited in claim 37 wherein combining is performed through an exclusive-OR (XOR) operation.

Claim 50 (new): The method recited in claim 33 wherein the data (X) comprises identification data of a payment device; and the processed data (Y) forms a diversified key.

Claim 51 (new): The method recited in claim 33 wherein the cryptographic process (P) comprises a DES process.

Claim 52 (new): The method recited in claim 51, wherein the DES process comprises triple DES.

Claim 53 (new): A circuit for performing the method recited in claim 33.

Claim 54 (new): A payment card having the circuit recited in claim 53.

Claim 55 (new): A payment terminal having the circuit recited in claim 53.

Claim 56 (new): The method recited in claim 34 wherein the data (X) comprises identification data of a payment device; and the processed data (Y) forms a diversified key.

Claim 57 (new): The method recited in claim 34 wherein the cryptographic process (P) comprises a DES process.

Claim 58 (new): The method recited in claim 57 wherein the DES process comprises triple DES.

Claim 59 (new): A circuit for performing the method recited in claim 34.

Claim 60 (new): A payment card having the circuit recited in claim 59.

Claim 61 (new): A payment terminal having the circuit recited in claim 59.

Claim 62 (new): The method recited in claim 36 wherein the data (X) comprises identification data of a payment device; and the processed data (Y) forms a diversified key.

Claim 63 (new): The method recited in claim 36 wherein the cryptographic process (P) comprises a DES process.

Claim 64 (new): The method recited in claim 63 wherein the DES process comprises triple DES.

Claim 65 (new): A circuit for performing the method recited in claim 36.

Claim 66 (new): A payment card having the circuit recited in claim 65.

Claim 67 (new): A payment terminal having the circuit recited in claim 65.